



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/801,684	03/17/2004	Hisanori Kawaura	250480US2	1875
22850	7590	07/24/2008	EXAMINER	
OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, P.C. 1940 DUKE STREET ALEXANDRIA, VA 22314			TRAORE, FATOUMATA	
			ART UNIT	PAPER NUMBER
			2136	
			NOTIFICATION DATE	DELIVERY MODE
			07/24/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

Office Action Summary	Application No.	Applicant(s)	
	10/801,684	KAWAURA ET AL.	
	Examiner	Art Unit	
	FATOUMATA TRAORE	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 07 May 2008.
 2a) This action is **FINAL**. 2b) This action is non-final.
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1,3-12,14-17,19-28 and 30-32 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) Claim(s) _____ is/are allowed.
 6) Claim(s) 1,3-12,14-17,19-28 and 30 is/are rejected.
 7) Claim(s) _____ is/are objected to.
 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.
 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
 3) Information Disclosure Statement(s) (PTO/SB/08)
 Paper No(s)/Mail Date 0122/2008.

4) Interview Summary (PTO-413)
 Paper No(s)/Mail Date. _____.
 5) Notice of Informal Patent Application
 6) Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 05/07/2008 has been entered. Claims 2, 13, 18 and 29 have been cancelled. Claims 1 12, 17, 28 have been amended. Claims 1, 3-12, 14-17, 19-28 and 30-32 are pending and have been considered below.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on 01/22/2008 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Response to Arguments

3. Applicant's arguments with respect to claims 1, 3-12, 14-17, 19-28 and 30-32 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 1, 3-11, 16, 19-27, 32 rejected under 35 U.S.C. 103(a) as being unpatentable over Hind et al (US 6976163) hereinafter Hind 163 in view of Hind et al (US ,990,444) hereinafter Hind 444.

Claim 1: Hind 163 discloses an apparatus for secure firmware update comprising:

- a. A storing unit configured to store a program in accordance with which the image forming apparatus operates (*the computer program instructions is stored in a computer- readable memory that directs a computer or other programmable data processing apparatus to function in a particular manner*) (*column 6, lines 36-40*);
- b. An acquiring unit configured to acquire an update program from an external source (*the computer program instruction is loaded onto a computer or other programmable data processing apparatus to cause a series of operational steps to be performed on the computer or other programmable apparatus to produce a computer implementation process*) (*column 6, lines 44-48; Fig. 3, Fig. 4, Fig. 10*); and

c. An updating unit that determines whether an electronic signature of the update program acquired by said acquiring unit is authentic and, if the electronic signature of the acquired update program is determined to be authentic (*the authenticity of the update image is verified. Such verification is accomplish in various ways for example by including a and checking a digital signature comprising a hash of the image encrypted by the private key of the an update authority*) (column 3, lines 18-30), updates the program stored in said storing unit using the acquired update program (*the programmable memory is updated with the update image only if all the update application rules indicate that the update image is applicable to the device*) (column 2, lines 53-60).

d. wherein the authentication of the update program is performed based on a message digest, the message digest being generated based on a configuration file of the update program and a unique identification of the external source (*the sender encrypts a signature message using the sender's private key, the signature messing being a hash or a message digest of the message being signed*) (column 3, lines 1-5; column 13, lines 23-35; column 15, lines 27-50; column 18, lines 13-60).

But Hind 163 does not explicitly disclose that the message digest being generated based on a configuration file of the update program and a unique identification of the external source. However, Hind 444 discloses an apparatus of doing business by providing improved audio stream, which further discloses

that the message digest being generated based on a configuration file of the update program and a unique identification of the external source (column 6, lines 7-35). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Hind 163 such as to include a step of authentication based on the a message digest generated based on configuration file and identification of the external source. One would have been motivated to do so in order to provide a technique whereby the authenticity and integrity of the encoded text stream can be verify as taught by Hind 444(Column 4, lines 57-60).

Claim 17: Hind 163 discloses an apparatus for secure firmware updates comprising:

- a. A storing unit that stores a program in accordance with which the image forming apparatus operates (*the computer program instructions is stored in a computer- readable memory that directs a computer or other programmable data processing apparatus to function in a particular manner*) (column 6, lines 36-40);
- b. An acquiring unit that acquires an update program from an external source (*the computer program instruction is loaded onto a computer or other programmable data processing apparatus to cause a series of operational steps to be performed on the computer or other programmable apparatus to produce a computer implementation process*) (column 6, lines 44-48); and

c. An updating unit that updates the program stored in said storing unit using the update program acquired by said acquiring unit, wherein after updating the program stored in said storing unit, said updating unit determines whether an electronic signature of the updated program is authentic and, if the electronic signature of the updated program is authentic (*the authenticity of the update image is verified. Such verification is accomplish in various ways for example by including a and checking a digital signature comprising a hash of the image encrypted by the private key of the an update authority*) (column 3, lines 18-30), said updating unit maintains the updated program (*the programmable memory is updated with the update image only if all the update application rules indicate that the update image is applicable to the device*) (column 2, lines 53-60).

d. wherein the authentication of the update program is performed based on a message digest, the message digest being generated based on a configuration file of the update program and a unique identification of the external source (*the sender encrypts a signature message using the sender's private key, the signature messing being a hash or a message digest of the message being signed*) (column 3, lines 1-5; column 13, lines 23-35; column 15, lines 27-50; column 18, lines 13-60).

But Hind 163 does not explicitly disclose that the message digest being generated based on a configuration file of the update program and a unique identification of the external source. However, Hind 444 discloses an apparatus

of doing business by providing improved audio stream, which further discloses that the message digest being generated based on a configuration file of the update program and a unique identification of the external source (column 6, lines 7-35). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Hind 163 such as to include a step of authentication based on the a message digest generated based on configuration file and identification of the external source. One would have been motivated to do so in order to provide a technique whereby the authenticity and integrity of the encoded text stream can be verify as taught by Hind 444(Column 4, lines 57-60).

Claims 3, 19: Hind 163 and Hind 444 disclose an apparatus for secure firmware updates as in claims 1 and 17 above, and Hind 163 further discloses that said updating unit updates the program stored in said storing unit with the update program acquired by said acquiring unit, and updates an electronic signature of the program stored in said storing unit with the electronic signature of the update program (*the update application rules defines how data from the update image is utilized to update the programmable memory and identifies installation information provided with the update image. The programmable memory would be updated utilizing the installation information by executing the install program to write the update data to the programmable memory*) (column 3, lines 5-17).

Claims 4, 20: Hind 163 and Hind 444 disclose an apparatus for secure firmware updates as in claims 1 and 17 above, and Hind 163 further discloses that said

acquiring unit is an update recording medium setting unit and the external source is an update recording medium to be set in the update recording medium setting unit, the update recording medium storing the update program and the electronic signature of the update program (*any suitable computer readable medium may be utilized including hard disk, CD-ROMs, optical storage devices, or magnetic storage devices*) (column 5, lines 50-53).

Claims 5, 21: Hind 163 and Hind 444 disclose an apparatus for secure firmware updates as in claims 1 and 17 above, and Hind 163 further discloses that said acquiring unit is a receiving unit that receives the update program and the electronic signature of the update program from the external source via a network (*the computer program is loaded onto a computer or other programmable data processing apparatus to cause a series of operational steps to be performed on the computer*) (column 6, lines 44-48).

Claims 6, 22: Hind 163 and Hind 444 disclose an apparatus for secure firmware updates as in claims 1 and 17 above, and Hind et al further discloses that said storing unit further comprises a recording medium setting unit and a recording medium set therein, the recording medium storing the program (these computer program instructions are also stored in a computer readable memory that can direct a computer and other programmable data processing apparatus to function in a particular manner) (column 6, lines 36-39).

Claims 7, 23: Hind 163 and Hind 444 disclose an apparatus for secure firmware updates as in claims 1 and 17 above, and Hind 163 further discloses:

An activating unit that determines whether the electronic signature of the update program and an electronic signature of a configuration file related to the update program are authentic and, if the electronic signature of the update program and the electronic signature of the configuration file related to the update program are determined to be authentic, activates the updated program (*the update image includes a plurality of certificates in a hierarchy of certificates. Authenticity of the update image is verified by evaluating each of the plurality of certificates in the update image to determine if a valid digital signature is provided with each certificate of the update image (update program and configuration file) (column 4, lines 4-10)*), Wherein said acquiring unit further acquires a configuration file and an electronic signature thereof from the external source (*the computer program instruction is loaded onto a computer or other programmable data processing apparatus to cause a series of operational steps to be performed on the computer or other programmable apparatus to produce a computer implementation process*) (*column 6, lines 44-48*); and said activating unit determines whether the electronic signature of the update program and the electronic signature of the configuration file are authentic and, if the electronic signature of the update program and the electronic signature of the configuration file are determined to be authentic, activates the update program in accordance with the configuration file (*the invention also provides a certificate for use in updating a programmable memory. Such certificate includes a digital signature and at least one extension having rules to control installation of an update image*).

A private key of a certificate authority signs the certificate. The programmable memories of generic processing devices is selectively update based on the distributed updates and the rules specified in the at least extension of the certificate. The sender encrypts a signature message using the sender's private key, the signature messing being a hash or a message digest of the message being signed) (column 12, lines 1-14, column , 12, lines 12-22).

Claims 8, 24: Hind 163 and Hind 444 disclose an apparatus for secure firmware updates as in claims 7 and 23 above, and Hind 163 further discloses that said activating unit determines whether the electronic signature of the update program is authentic by comparing a message digest generated from the update program and a message digest obtained by decrypting the electronic signature of the update program (*the verification of signature is provided by computing the hash over the image, decrypting the signature using the public key from the included certificate, and comparing the decrypt result with the computed hash value*) (column 3, lines 33-36).

Claims 9, 25: Hind 163 and Hind 444 disclose an apparatus for secure firmware updates as in claims 7 and 23 above, and Hind 163 further discloses that said activating unit determines whether the electronic signature of the configuration file is authentic by comparing a message digest generated from the configuration file and a message digest obtained by decrypting the electronic signature of the configuration file (*the verification of signature is provided by computing the hash over the image, decrypting the signature using the public key from the included*

certificate, and comparing the decrypt result with the computed hash value)
(column 3, lines 33-36).

Claims 10, 26: Hind 163 and Hind 444 disclose an apparatus for secure firmware updates as in claims 9 and 25 above, Hind 163 further discloses that that the electronic signature of the configuration file is generated by encrypting a message digest of the configuration file and identification information of the recording medium (the sender encrypts a signature message using the sender's private key, the signature message being a hash or a message digest of the message being signed) (column 12, lines 1-14, column , 12, lines 12-22)

Claims 11, 27: Hind 163 and Hind 444 disclose an apparatus for secure firmware updates as in claims 10 and 26 above, and Hind 444 further discloses that the identification information of the recording medium is a serial ID of the recording medium.(column 11, lines 65-67) Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of to Hind 163 such as to include a step of authentication based on the a message digest generated based on configuration file and identification of the external source. One would have been motivated to do so in order to provide a technique whereby the authenticity and integrity of the encoded text stream can be verify as taught by Hind 444(Column 4, lines 57-60).

Claims 16, 32: Hind 163 and Hind 444 disclose an apparatus for secure firmware updates as in claims 4 and 20 above, and Hind 163 further discloses that the update recording medium storing the update program and the electronic

signature thereof (the update application rules defines how data from the update image is utilized to update the programmable memory and identifies installation information provided with the update image. The programmable memory would be updated utilizing the installation information by executing the install program to write the update data to the programmable memory) (column 3, lines 5-17).

6. Claims 12, 14, 15, 28, 30, 31 rejected under 35 U.S.C. 103(a) as being unpatentable over Mattison (US 6615355) in view of Hind et al (US ,990,444) hereinafter Hind 444.

Claim 12: Mattison discloses a method for protecting flash memory from any unauthorized reprogramming effort comprising:

- a. Acquiring an update program and an electronic signature corresponding to the update program (*a flash memory upgrade program containing a new flash memory image for the flash memory would be loaded into main system memory*) (column 3, lines 25-27);
- a. Determining whether the acquired electronic signature of the update program is authentic (comparing the original hash value obtained from decrypting the digital signature with the independently generated hash value to find a match) (column 3, lines 51-54); and
- b. Updating, if the acquired electronic signature of the acquired update program is determined to be authentic, the program stored in the recording medium using the acquired update program (*if the hash values*

match, indicating that flash memory upgrade program containing in main memory originated from the authorized creator and has not been modified, then the current program containing in the lash memory would enable reprogramming of the flash memory and return control of the processor to the flash memory upgrade program) (column 3, lines 55-61).

c. wherein the authentication of the update program is performed based on a message digest, the message digest being generated based on a configuration file of the update program and a unique identification of the external source (*the sender encrypts a signature message using the sender's private key, the signature messing being a hash or a message digest of the message being signed) (column 3, lines 1-5; column 13, lines 23-35; column 15, lines 27-50; column 18, lines 13-60).*

But Mattison does not explicitly disclose that the message digest being generated based on a configuration file of the update program and a unique identification of the external source. However, Hind 444 discloses an apparatus of doing business by providing improved audio stream, which further discloses that the message digest being generated based on a configuration file of the update program and a unique identification of the external source (column 6, lines 7-35). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Hind 163 such as to include a step of authentication based on the a message digest generated based on configuration file and identification of the external source.

One would have been motivated to do so in order to provide a technique whereby the authenticity and integrity of the encoded text stream can be verify as taught by Hind 444(Column 4, lines 57-60).

Claim 28: Mattison discloses a method for protecting flash memory from any unauthorized reprogramming effort comprising:

a. Acquiring an update program from an external source (a flash memory upgrade program containing a new flash memory image for the flash memory would be loaded into main system memory) (column 3, lines 25-27);

Updating the program stored in the recording medium using the acquired update program (the flash memory upgrade would then erase the flash memory and copy the new flash memory image into the flash memory) (column 3. lines 62- 64);

b. Determining whether an electronic signature of the updated program is authentic (*comparing the original hash value obtained from decrypting the digital signature with the independently generated hash value to find a match*) (column 3, lines 51-54); and

c. Maintaining, if the electronic signature of the updated program is determined to be authentic, the updated program (*if the hash values match, indicating that flash memory upgrade program containing in main memory originated from the authorized creator and has not been modified, then the current program containing in the lash memory would enable*

reprogramming of the flash memory and return control of the processor to the flash memory upgrade program) (column 3, lines 55-61).

d. wherein the authentication of the update program is performed based on a message digest, the message digest being generated based on a configuration file of the update program and a unique identification of the external source (*the sender encrypts a signature message using the sender's private key, the signature message being a hash or a message digest of the message being signed*) (column 3, lines 1-5; column 13, lines 23-35; column 15, lines 27-50; column 18, lines 13-60).

But Mattison does not explicitly disclose that the message digest being generated based on a configuration file of the update program and a unique identification of the external source. However, Hind 444 discloses an apparatus of doing business by providing improved audio stream, which further discloses that the message digest being generated based on a configuration file of the update program and a unique identification of the external source (column 6, lines 7-35). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Hind 163 such as to include a step of authentication based on the a message digest generated based on configuration file and identification of the external source. One would have been motivated to do so in order to provide a technique whereby the authenticity and integrity of the encoded text stream can be verify as taught by Hind 444(Column 4, lines 57-60).

Claims 14, 30: Mattison and Hind 444 disclose a method for protecting flash memory from any unauthorized reprogramming as in claims 12 and 28, and Mattison further discloses that if the step of acquiring electronic signature of the update program is determined to be authentic, an electronic signature of the program stored in the recording medium is updated together with the program stored in the recording medium (*the flash memory upgrade would then erase the flash memory and copy the new flash memory image into the flash memory*) (column 3, lines 62-64).

Claims 15, 31: Mattison and Hind 444 disclose a method for protecting flash memory from any unauthorized reprogramming effort as claimed in claims 12 and 28 above, and Mattison further discloses a step of activating, if the acquired electronic signature of the acquired update program and an acquired electronic signature of an acquired configuration file are determined to be authentic, the updated program in accordance with the acquired configuration file (*the flash memory upgrade program, still executing from main system memory, would then transfer control of the processor to the program containing in the new flash memory image, now in flash memory, which in turn would return the memory controller to normal operation and begin its normal initialization sequence as if a reset had occurred*) (column 4, lines 13-20).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571) 270-1685. The examiner can normally be reached Monday through Thursday from 7:00 a.m. to 4:00 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nassar G. Moazzami, can be reached on (571) 272 4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is (571) 273-8300. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 270-2685.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

FT

Friday, July 18, 2008

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2136